



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

CBRN-security begint met een zelfanalyse

Inleiding

Betere beveiliging van chemische, biologische, radiologische en nucleaire (CBRN) stoffen begint met een goede zelf-analyse. Deze folder geeft basisinformatie over risico's van CBRN-stoffen en beveiligingsmaatregelen die daaraan gekoppeld zijn. Met de uitgebreidere Zelfanalysemodule CBRN Security kunt u vervolgens bepalen of bestaande maatregelen bij uw organisatie de risico's afdoende afdekken of dat aanvullende maatregelen nodig zijn.

Waarom beveiligingsmaatregelen?

De hedendaagse maatschappij kan niet zonder onderzoek en de toepassing en uitwisseling van innovatieve technologieën. Als

gevolg daarvan zijn chemische, biologische, radiologische en nucleaire stoffen en daaraan verbonden kennis en informatie in Nederland gemeengoed. Deze stoffen zijn voor kwaadwillenden echter ook interessante middelen om een aanslag mee te plegen. Hoewel een grote CBRN-aanslag niet waarschijnlijk is, kan ook een weinig effectieve aanslag met CBRN-stoffen of een poging daartoe leiden tot maatschappelijke onrust.

Daarom is het belangrijk om beveiligingsmaatregelen te nemen. Deze maatregelen beschermen tegen moedwillige incidenten – zoals diefstal, sabotage of een aanslag – en worden ook wel aangeduid met de term security. Dit is iets anders dan safety, dat slaat op bescherming tegen incidenten die het gevolg zijn van niet-moedwillig handelen, technisch falen of natuurgeweld.

Afhankelijk van het risiconiveau van een stof moet met diverse dreigingsscenario's rekening worden gehouden. Voorbeelden daarvan zijn:

- Binnendringen van één of meerdere personen bij een organisatie met als doel diefstal van CBRN-stoffen.
- Diefstal van informatie of informatiedragers die toegang verschaft tot CBRN-stoffen.
- Afluisteren van gesprekken en/of communicatie-apparatuur om toegang te krijgen tot CBRN-stoffen.
- Fraude in de vorm van leveren van CBRN-stoffen aan niet geautoriseerde personen of fraude via ongeautoriseerde aankoop buiten de registratie om.
- Overval op transport of tijdens mobiel gebruik van CBRN-stoffen.
- Ontvoering, afpersing, of omkoping van personeel, met als doel het verwerven van (kennis over) toegang tot CBRN-stoffen.
- Sabotage van bedrijfsprocessen waardoor stoffen vrijkomen in de lucht.
- Explosie om toegang te verschaffen tot CBRN-stoffen of deze te verspreiden.



Wat zijn CBRN-stoffen?

'CBRN' staat voor chemische, biologische, radiologische en nucleaire stoffen, die een risico vormen voor de volksgezondheid en/of voor het milieu:

Chemische stoffen

Stoffen zoals toxische chemicaliën, pesticiden en chemische strijdmiddelen.

Biologische stoffen

Stoffen die als ziekteverwekker optreden voor mens, plant of dier (humaanpathogenen, dierpathogenen en plantpathogenen).

Radiologische stoffen

Stoffen die een risico vormen in het geval van interne of externe blootstelling aan hun straling.

Nucleaire stoffen

Stoffen zoals plutonium, uranium-233 en uranium verrijkt met isotoop 235 of 238.

Richtlijnen voor CBRN-security

In 2006 heeft de Nationaal Coördinator Terrorisme-bestrijding en Veiligheid (NCTV) van het ministerie van Veiligheid en Justitie samen met een aantal overheidspartijen een raamwerk ontwikkeld met richtlijnen voor CBRN-security. Deze richtlijnen zijn opgenomen in het vertrouwelijke 'Normatief format van beveiligingsafspraken voor CBRN-onderzoeksinstituten'. Deze richtlijnen beslaan twee delen: (1) het inschatten van het risiconiveau van de organisatie en (2) het bepalen en uitvoeren van de noodzakelijke maatregelen. Een groot deel van deze richtlijnen is toepasbaar op alle organisaties die werken met CBRN-stoffen. Dat kan een ziekenhuis, een universiteit, een laboratorium of een chemisch bedrijf zijn. Dat laat onverlet dat iedere organisatie uniek is en dat maatregelen dus per organisatie zullen verschillen. Voor organisaties met een open (publiek) karakter is het bijvoorbeeld lastiger om toegangsbeperkende maatregelen te nemen dan voor vertrouwelijke en gesloten omgevingen; dan kunnen andere maatregelen, zoals het zoneren van activiteiten en het beveiligen van gevoelige onderdelen van de organisatie, nodig zijn.

Deel 1: Het risiconiveau inschatten

De aanwezige stoffen op een locatie bepalen het risiconiveau van een organisatie. De impact die deze stoffen kunnen hebben bij een terroristische of criminele aanslag bepalen voor een groot deel het risiconiveau van een organisatie: stoffen met ernstige gevolgen en/of een groot effectgebied leveren grotere risico's op dan stoffen met beperkte gevolgen en/of een beperkt effectgebied. Daarnaast leveren stoffen die qua toepassing moeilijker zijn kleinere risico's op dan stoffen die eenvoudig te verspreiden zijn. Onderstaande tabel beschrijft drie risiconiveaus: Basis, Midden en Hoog. De beschrijvingen zijn in dit document veralgemeniseerd. Meer gedetailleerde informatie is te vinden in de Zelfanalysemodule CBRN Security.

Basis	Een terroristische of criminele aanslag met een stof uit deze categorie heeft in een klein gebied beperkte gevolgen voor de volksgezondheid en/of het milieu. Uw organisatie heeft in ieder geval een basis risiconiveau als u werkt met één of meer van de volgende stoffen: <i>Chemische stoffen</i> • Een kleine hoeveelheid van een toxische vloeistof. • Een pesticide voorzien van de waarschuwingszin “giftig bij aanraking met de huid”. <i>Biologische stoffen</i> • Sommige pathogenen die bij de mens een ziekte kunnen veroorzaken. • Sommige pathogenen die bij dieren een (ernstige) ziekte kunnen veroorzaken. <i>Radiologische / nucleaire stoffen</i> • Kunstmatige radioactieve stoffen ten behoeve van: - hoogactieve vaste industriële meetapparatuur - bemetingsapparatuur t.b.v. olie- en gaswinning (well logging) • Overige kunstmatige radioactieve stoffen waarvan: $10 > A/D > 1$ (zie uitvoeringsregeling stralingsbescherming EZ en IAEA D-waarden).
Midden	Een terroristische of criminele aanslag met een stof uit deze categorie heeft in de directe en indirecte omgeving grote gevolgen voor de volksgezondheid en een grote psychologische impact. Daarnaast kan een aanslag tot milieuschade leiden. Uw organisatie heeft in ieder geval een midden risiconiveau als u werkt met één of meer van de volgende stoffen: <i>Chemische stoffen</i> • Een aanzienlijke hoeveelheid van een toxische vloeistof. • Een kleine hoeveelheid van een toxisch gas. • Een pesticide voorzien van de waarschuwingszin “giftig bij inademing”, “giftig bij opnemning door de mond” of “zeer giftig bij aanraking met de huid”. <i>Biologische stoffen</i> • Sommige pathogenen die bij de mens een ernstige ziekte kunnen veroorzaken. • Sommige pathogenen die bij dieren een (zeer) ernstige ziekte kunnen veroorzaken. • Een plantpathogeen met potentieel grote economische impact. <i>Radiologische / nucleaire stoffen</i> • Kunstmatige radioactieve stoffen ten behoeve van: - industriële gammagrafie - brachytherapie (stralingsdosistempo van 2,0 Gy of hoger) • Overige kunstmatige radioactieve stoffen waarvan: $1000 > A/D > 10$ (zie uitvoeringsregeling stralingsbescherming EZ en IAEA D-waarden). • Nucleair materiaal in IAEA Nuclear Material Category III. Uw organisatie heeft ook een midden risiconiveau indien gedetailleerde informatie en kennis over de vervaardiging, toepassing en verspreiding van bovengenoemde stoffen aanwezig is.
Hoog	Een terroristische of criminele aanslag met een stof uit deze categorie heeft in een groot gebied grote gevolgen voor de volksgezondheid en een grote psychologische impact. Daarnaast kan een aanslag tot grote milieuschade leiden. Uw organisatie heeft in ieder geval een hoog risiconiveau als u werkt met één of meer van de volgende stoffen: <i>Chemische stoffen</i> • Een chemisch strijdmiddel of een voorloper daarvan. • Een grote hoeveelheid van een toxische vloeistof. • Een grote hoeveelheid van een toxisch gas. • Een pesticide voorzien van de waarschuwingszin “zeer giftig bij inademing” of “zeer giftig bij opnemning door de mond”. <i>Biologische stoffen</i> • Sommige pathogenen die bij de mens een ernstige ziekte kunnen veroorzaken en waarvan er een (grote) kans is dat deze zich onder de bevolking verspreiden. • Sommige pathogenen die bij dieren een zeer ernstige ziekte kunnen veroorzaken. • Een plantpathogeen met potentieel zeer grote economische impact. <i>Radiologische / nucleaire stoffen</i> • Kunstmatige radioactieve stoffen ten behoeve van: - nucleaire batterijen - sterilisatie, onderzoek en bloedbestraling - teletherapie apparatuur - vaste, multibundel teletherapie • Overige kunstmatige radioactieve stoffen waarvan: $A/D > 1000$ (zie uitvoeringsregeling stralingsbescherming EZ en IAEA D-waarden). • Nucleair materiaal in IAEA Nuclear Material Category I en II. Uw organisatie heeft ook een hoog risiconiveau indien gedetailleerde informatie en kennis over de vervaardiging, toepassing en verspreiding van bovengenoemde stoffen aanwezig is.

Deel 2: Maatregelen bepalen en uitvoeren

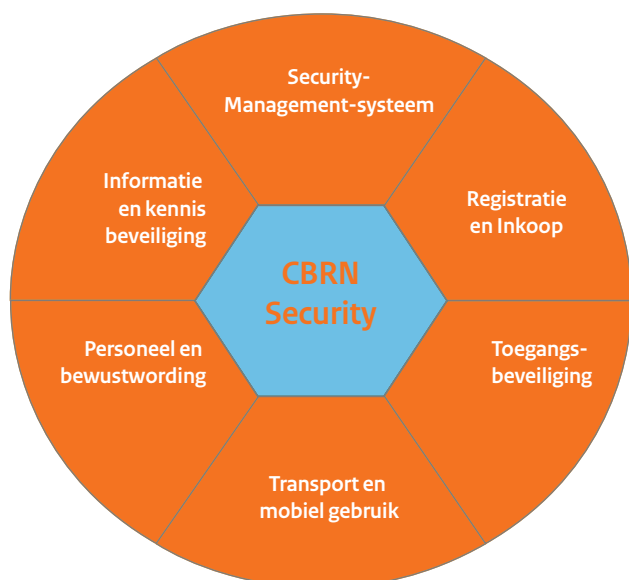
Op basis van het risiconiveau wordt bepaald welke maatregelen nodig zijn voor de beveiliging van CBRN-stoffen en informatie/kennis over deze stoffen. De NCTV richtlijnen voor CBRN security beschrijven maatregelen binnen zes thema's:

Security-Managementsysteem

Een security-managementsysteem is een bedrijfsvoeringssystematiek, die gebruikt wordt om security binnen de organisatie inzichtelijk en effectief te maken. Het is een geïntegreerde, risicogeorïënteerde benadering met een gestructureerde, systematische kijk op de beveiliging van de organisatie. Hiermee krijgt een organisatie grip op security-risico's en kan zij weloverwogen maatregelen nemen om deze te verkleinen. Hierdoor is de organisatie permanent voorbereid op moedwillige aantasting van waardevolle bedrijfsprocessen en objecten. Security management bestaat uit een aantal periodieke activiteiten:

- Het uitvoeren van object- en procesanalyses.
- Het uitvoeren van risicoanalyses.
- Het opstellen van security-beleid.
- Het benoemen van taken, verantwoordelijkheden en bevoegdheden.
- Het meten en verbeteren van de prestatie van de beveiliging.

Dit alles gebeurt via een zogenoemde Plan Do Check Act-cyclus.



Voorbeelden van security-management bij een basis, midden of hoog risiconiveau

Van alle organisaties die werken met CBRN-stoffen wordt verwacht dat ze beschikken over een up-to-date security-managementsysteem. De richtlijn vraagt daarbij van organisaties die werken met stoffen met een midden- of hoog risico om dit security-managementsysteem te integreren met het safety-managementsysteem en eindverantwoordelijken en uitvoeringsverantwoordelijken voor security vast te stellen. Organisaties die werken met stoffen met een hoog risico moeten daarnaast ook werken op basis van een gedetailleerd dreiging- en risicobeoordelingsproces.

Registratie en inkoop

Maatregelen voor registratie en inkoop van CBRN-stoffen zijn essentieel voor goed beheer van deze stoffen. Een deugdelijke registratie van voorraden en autorisaties draagt bij aan de algehele beveiliging van CBRN-stoffen: op ieder moment is inzichtelijk welke stoffen aanwezig zijn in de organisatie en wie ermee werkt. Ook inkoop moet op een gecontroleerde en geautoriseerde wijze plaatsvinden, waardoor zicht is op aanschaf van specifieke stoffen.

Voorbeelden van registratie en inkoop bij een basis, midden of hoog risiconiveau

Van alle organisaties die werken met CBRN-stoffen wordt verwacht dat zij een actuele lijst hebben van alle stoffen, inclusief de opslag- en gebruikslocaties. Van organisaties die werken met stoffen met een midden- of hoog risico wordt verwacht dat zij bij het inkoopproces monitoren of en in welke context deze stoffen worden aangeschaft. Voor stoffen met een hoog risico moet er van aankoop tot afvoer adequaat beheer zijn van de stoffen ('chain of custody').

Toegangsbeveiliging

Goede toegangsbeveiliging (vaak ook fysieke beveiliging genoemd) bestaat uit bouwkundige en elektronische afscherming en detectie van CBRN-stoffen.

Beveiligingsmaatregelen zoals sloten, paslezers, afsluitbare kasten en zonering van activiteiten moeten de toegang tot CBRN-stoffen binnen de organisatie beveiligen.

Beveiligingsmaatregelen zoals camera's en het registreren van toegang moeten ongeautoriseerde toegang en/of vermissing van bepaalde stoffen zo snel mogelijk detecteren.

Voorbeelden van toegangsbeveiliging bij een basis, midden of hoog risiconiveau

Van alle organisaties die werken met CBRN-stoffen wordt verwacht dat zij deze stoffen zorgvuldig opslaan. Van organisaties die werken met stoffen met een midden- en hoog risico wordt verwacht dat zij de toegang tot deze stoffen autoriseren en controleren. Toegang tot stoffen met een hoog risico wordt door minimaal twee beveiligingsbarrières beveiligd.

Transport en mobiel gebruik

CBRN-stoffen staan niet altijd op dezelfde plaats. CBRN-stoffen zijn kwetsbaarder tijdens transport of 'mobiel gebruik'. Interne en externe transporten vragen dan ook om specifieke beveiligingsmaatregelen, zoals afsluitbare transportkarren en goede uit- en incheckprocedures.

Voorbeelden van transport en mobiel gebruik bij een basis, midden of hoog risiconiveau

Voor het transport en mobiel gebruik van CBRN-stoffen geldt dat deze zo snel mogelijk weer in de beveiligde omgeving van de vaste locatie moeten worden opgeborgen. Voor het transport en mobiel gebruik van stoffen met een midden- en hoog risico moet altijd bekend zijn waar en wanneer dit plaatsvindt; deze stoffen mogen niet onbeheerd achter worden gelaten. Stoffen met een hoog risico moeten zich altijd in een bewaakte omgeving bevinden of beschermd worden. Zij moeten ook op elk moment traceerbaar zijn.

Personeel en bewustwording

Zonder personele maatregelen en goede security-cultuur is er geen CBRN-security. Alerte medewerkers, een alert management en alerte veiligheidsprofessionals zijn essentieel om (de dreiging van) mogelijke criminele, frauduleuze of terroristische activiteiten tijdig te herkennen. Bewustwordingstrainingen over security versterken de zwakste schakel in een goed security systeem. Ook onderkenning van risicofuncties en een helder screeningsbeleid zijn voorwaarden voor het veilig omgaan met CBRN-stoffen.

Voorbeelden van personeel en bewustwording bij een basis, midden of hoog risiconiveau

Alle medewerkers met toegang tot CBRN-stoffen dienen een bewustwordingstraining over CBRN-security te hebben gevolgd. Organisaties die werken met CBRN-stoffen moeten daarnaast risicofuncties benoemen en een screeningsbeleid opstellen. Het niveau van screening hangt af van het risico dat een functie met zich meebrengt. Als vuistregel kan aangehouden worden:

- Werken met stoffen met een basis risico: minimaal een Verklaring Omtrent het Gedrag (VOG) of vergelijkbare screening voor alle medewerkers met toegang.
- Werken met stoffen met een midden risico: minimaal een Verklaring Omtrent het Gedrag (VOG) of vergelijkbare screening voor alle medewerkers en externen met toegang.
- Werken met stoffen met een hoog risico: een Verklaring van Geen Bezwaar (VGB) of vergelijkbare screening voor alle medewerkers met toegang en een VOG voor alle externen.

Informatie- en kennisbeveiliging

Informatie over de aanwezigheid of beschikbaarheid van CBRN-stoffen is vaak de eerste stap naar toegang tot deze stoffen. Deze informatie en kennis moeten daarom goed beveiligd worden, door onder meer de beveiliging van digitale opslag en de toegang tot ICT-systemen. Ook informatie over de vervaardiging van chemische, biologische of nucleaire wapens dient goed beveiligd te zijn om proliferatie van deze informatie te voorkomen.

Voorbeelden van informatie- en kennisbeveiliging bij een basis, midden of hoog risiconiveau

Alle organisaties die werken met CBRN-stoffen moeten beschikken over een gedegen informatiebeveiligingsbeleid dat voorkomt dat ongeautoriseerden toegang hebben tot informatie en kennis. Dit betreft ook digitale beveiliging zoals het hebben van up-to-date firewalls, virusscanners en software en het periodiek vervangen van wachtwoorden. Organisaties die werken met stoffen met een midden- en hoog risico voeren periodiek een afhankelijkheids- en kwetsbaarheidsanalyse uit voor de aanwezige informatie en hun ICT-systeem. Daarnaast wordt informatie geclassificeerd zodat vertrouwelijke informatie alleen beschikbaar is voor een geselecteerde groep medewerkers.

Gebruik de Zelfanalysemodule CBRN Security

Hierboven is een overzicht gegeven van risiconiveaus en maatregelen. Bent u benieuwd hoe uw organisatie ervoor staat? Dan kunt u gebruik maken van de Zelfanalysemodule CBRN Security. Deze module is speciaal ontwikkeld voor bedrijven en publieke instellingen die werken met CBRN-stoffen. Met deze module krijgt u snel een globaal inzicht in de staat van de beveiliging van deze stoffen bij uw organisatie. Daarnaast bevat zij tips van andere organisaties om uw beveiliging te verbeteren. De module is ontwikkeld door NCTV in samenwerking met een groot aantal experts vanuit de overheid, de chemiesector, en onderzoeksinstellingen.

De Zelfanalysemodule CBRN Security bestaat uit drie stappen: een risicoanalyse, een thematische vragenlijst en een resultatenpagina:

Stap 1. Risico-analyse

U bepaalt welk type CBRN-stoffen er binnen uw organisatie aanwezig zijn. Daarnaast stelt u op basis van het type aanwezige stoffen en de beschikbare hoeveelheden vast wat het risiconiveau van uw organisatie is.

Stap 2. Thematische vragenlijst

Door middel van vragen binnen de zes bovengenoemde thema's wordt inzicht gegeven in de staat van de beveiliging van uw CBRN-stoffen.

Stap 3. Resultatenpagina

Tot slot worden de resultaten gepresenteerd in een spinnenweb-diagram. Op basis van de verstrekte informatie, wordt per thema gevisualiseerd wat het huidige weerstandsniveau van uw organisatie is. Per thema worden verschillende tips en verwijzingen naar websites gegeven die u op het betreffende onderwerp verder kunnen informeren.

De volgende stap is aan uzelf: gebruik de verzamelde informatie en aangereikte tips om CBRN-security en de weerbaarheid van uw organisatie verder te verbeteren.



